Oracle Insight

State of Montana Identity Management Strategy Discovery Map - DRAFT 2

Vision / Goals

Create a state-wide identity management strategy that promotes operational efficiencies and enhances security and accountability

Key Business Requirements

- Drive consistent standard levels of security and identity management practices across MT
- "One stop shopping" for provisioning, modifying, removing and auditing access
- Promote usability of technology while maintaining proper levels of security
- Ensure accountability with comprehensive and robust audit capabilities
- Maintain security of sensitive citizen, employee and business information
- Ensure scalable, flexible, agile and open technology and systems
- Promote Green practices
- Utilize technology and improved processes to gain cost efficiencies
- Promote government transparency with citizen self-service capabilities
- Share information internally and externally with appropriate access and audit controls
- Be more proactive and less reactive
- Comply with privacy and internal control laws and policies

Consequential Pains

User Life Cycle Management (Provisioning / De-provisioning)

- On-boarding process taking up to 2 weeks to complete
- Potential for assignment of incorrect access levels
- Difficult to audit or enforce accountability
- High paper process not meeting Green Initiative goals
- End user frustration
- Terminated contractors retain access to critical systems
- New employees are not immediately productive
- Possible accumulative privileges during role change
- Access to critical systems & facilities retained after role change / termination
- Sensitive citizen employee & business information is at risk
- Inconsistent access privileges granted to employee type
- Highly skilled employees conducting tedious low-level tasks
- External users may retain access longer than necessary
- High Help Desk costs
- Potential for untraceable internal rouge activity
- Manual account setup prone to data entry errors
- Provisioning of access is often incomplete
- High cost of provisioning / de-provisioning
- Sensitive information is vulnerable
- Provisioning process knowledge may be lost with retirements
- Overhead of security and general mgmt. of citizen identities

Access / Asset / Audit Management

- High costs of managing multiple identity repositories
- No single trusted store of access information
- No single place to see user access
- Hard to complete e-discovery requests
- Potential for identity mistakes and unauthorized access
- Hard to retrieve physical assets after employee termination
- Incomplete user off-boarding
- Unable to preform root cause analysis to prevent a repeat incident
- Difficult to audit or enforce accountability
- Not always meeting auditing & privacy laws or policy requirements
- Potential for security breeches from orphaned accounts
- Not able to provide information about breech to public
- Identity fragmentation from multiple repositories
- Users having access to data that are not part of job responsibilities
- Legal liability can not shed in case of unauthorized / inappropriate activity

Authentication

- Up to 40% of Help Desk calls are for password assistance
- Reduced security of critical applications and sensitive data
- Difficult to meet 20x10 initiative (mobile / tele-worker)
- Increased risk of remote intrusions
- User frustration
- Additional work to change common / shared passwords after employee leaves
- Lost productivity
- Potential loss of access to Federal systems

Tactical Pains

User Life Cycle Management (Provisioning / De-provisioning)

- Manual, paper-based/email process for on-boarding 2
- Application level accounts are not always removed ("Ghost Accounts") 2
- Inter-agency moves often results in new ID assigned 2
- Last name change results in lost application history / prefs. 3
- Estimated up to 50% of contractors retain VPN access after termination 1
- Reliance on supervisor for off-boarding 2
- Role changes are a manual paper-based process 1
- Inconsistent or undocumented provisioning process 1
- 10-15 people can be involved with provisioning process 1
- Reuse of IDs 2
- Application history is lost during role change 2
- No consistent process for provisioning / de-provisioning external users 1
- Rely on biyearly database activity reports to remove users 2
- No automated account management workflow 1
- Most positions do not have roles or access rights pre-defined 2
- Up to 2 weeks for de-provision notifications to arrive 1
- Expected increased amount of citizen online access 1
- Limited role based access management 2
- De-Provisioning is manual process that can take 5-8 hours 2
- No self-service / supervisor account request / provisioning system 1
- No consistent way of interacting with ITSD for access requests 1

Access / Asset / Audit Management

- Incomplete paper-based access list management 1
- High number of users stores 1
- Lack of preventative encryption of sensitive data 1
- Terminated employees access history is often lost 1
- High number of orphaned accounts 2
- Limited separation of duties 1
- Physical access system is not integrated with logical access systems 2
- Inconsistent security policy enforcement 1
- No centralized, secured, or consistent app auditing repository 1
- Few systems have consistent or proactive access / activity auditing 1
- AUP is outdated and not retained for auditing and attestation 2
- Lack of knowledge or enforcement of auditing/privacy legal / policies 1
- No centralized physical asset inventory management 2
- Limited proactive on consistent intrusion / misuse detection 1

Authentication

- Users have many different logins/passwords across systems 2
- Trusted authentication not possible 2
- Passwords are not synced 2
- Social engineering can be used for password resets 2
- No consistent password requirements 2
- Passwords being shared by users 1
- Users writing down passwords on Post-It notes 2
- Not able to comply with Federal password requirements 2
- No password self-reset 1

1 - **High** Business Impact
2 - **Medium** Business Impact
3 - **Low** Business Impact